IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	:	
	:	Group Art Unit: 2134
Michael G. LEE et al.	:	
	:	Examiner: Andrew L. Nalven
Appln. No.: 09/865,667	:	
	:	Confirmation No.: 4126
Filed: May 29, 2001	:	
	:	Customer No.: 21967
For: METHOD AND APPARATUS FOR SECURELY TRANSMITTING ENCRYPTED DATA THROUGH A FIREWALL AND FOR MONITORING USER TRAFFIC	:	

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is submitted in response to the Notice of Non-Compliant Appeal Brief filed April 20, 2007. The Office alleges that the Appeal Brief filed September 21, 2006 is deficient because it "fails to identify and map[] all independent claims on appeal (1, 4, 5, 7, 10 & 11) to specification by page and line number or paragraph number and/or drawings." Accordingly, in the Summary of the Claimed Invention of this Appeal Brief, concise explanations of each of the independent claims are provided, including reference to

exemplary portions of the specification and figures as required by 37 C.F.R. 41.37(c)(1)(v).

REAL PARTY IN INTEREST

The Appellants, Michael G. Lee and Leslie D. Owens, are the Applicants in the above-identified patent application. The Appellants have assigned their entire interest in the above-identified patent application to Nortel Networks Limited, 2351 Boulevard Alfred-Nobel, St. Laurent, Quebec, H4S 2A9 Canada.

RELATED APPEALS AND INTERFERENCES

The Appellants, the Appellants' legal representative, and the Assignee are not aware of any other appeals or interferences which will directly affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

STATUS OF CLAIMS

Claims 1-12 are pending in the above-identified patent application. Claims 1-12 were finally rejected in an Office Action dated February 28, 2006. The final rejection of Claims 1-12 is hereby appealed.

Claims 1, 2, 4-8, and 10-12 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Perlman et al. (U.S. Patent No.

6,546,486). Claims 3 and 9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Perlman et al. (U.S. Patent No. 6,546,486) in view of Ylonen et al. (U.S. Patent No. 6,438,612).

STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection of claims 1-12 in the Office Action dated February 28, 2006.

SUMMARY OF THE CLAIMED INVENTION

The claimed invention, as set forth in claim 1, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, is directed to a method for enabling a firewall to securely pass encrypted data (page 6, lines 3-5). The method may comprise detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (page 6, lines 5-10). The method may also comprise exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the

exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy (page 6, lines 13-19). The method may further comprise requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy (page 6, lines 19-23). The method may still further comprise passing encrypted data when it is determined that the first encryption key is received (page 6, lines 23-25).

The claimed invention, as set forth in claim 2, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, may be further defined by not allowing encrypted data to pass when it is determined that the first encryption key is not received.

The claimed invention, as set forth in claim 3, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, may be further defined by the step of detecting an exchange of a first encryption key further comprising monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged.

The claimed invention, as set forth in claim 4, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, is also directed to a method for enabling a firewall to selectively monitor encrypted data traffic (page 7, lines 1-3). The method may comprise detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key enables confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (page 7, lines 3-8). The method may also comprise exchanging a second encryption key with the host device when the exchange of the first key is detected, wherein the exchange of the second encryption key enables confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy (page 7, lines 8-14). The method may further comprise requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy (page 7, lines 14-18). The method may still further comprise decrypting encrypted data, using the first encryption key, according to a predetermined monitoring

policy (page 7, lines 18-21).

The claimed invention, as set forth in claim 5, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, is also directed to a method for enabling a firewall to selectively pass protocols and services (page 7, lines 22-24). The method may comprise detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (page 7, line 24 to page 8, line 4). The method may also comprise exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy (page 8, lines 4-10). The method may further comprise requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy (page 8, lines 10-14). The method may still further comprise decrypting encrypted data, using the

first encryption key (page 8, lines 15-18). The method may still further comprise applying a predetermined filtering policy to the decrypted data (page 8, lines 15-18).

The claimed invention, as set forth in claim 6, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, may be further defined by re-encrypting the decrypted data.

The claimed invention, as set forth in claim 7, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, is also directed to a firewall apparatus that securely passes encrypted data (page 6, lines 3-5). The apparatus may comprise an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (page 6, lines 5-10). The apparatus may also comprise a key exchanger for exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security

policy (page 6, lines 13-19). The apparatus may further comprise a key requestor for requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy (page 6, lines 19-23). The apparatus may still further comprise an encrypted data passer for passing encrypted data when it is determined that the first encryption key is received (page 6, lines 23-25).

The claimed invention, as set forth in claim 8, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, may further comprise an encrypted data blocker for not allowing encrypted data to pass when it is determined that the first encryption key is not received.

The claimed invention, as set forth in claim 9, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, may be further defined by the exchange detector further comprising a monitor for monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged.

The claimed invention, as set forth in claim 10, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, is also directed to a firewall apparatus for selectively monitoring encrypted data traffic (page 7, lines 1-3). The apparatus may comprise an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key enables confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (page 7, lines 3-8). The apparatus may also comprise a key exchanger for exchanging a second encryption key with the host device when the exchange of the first key is detected, wherein the exchange of the second encryption key enables confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy (page 7, lines 8-14). The apparatus may further comprise a requestor for requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy (page 7, lines 14-18). The apparatus may still further comprise a decryptor for decrypting encrypted data, using the

first encryption key, according to a predetermined monitoring policy (page 7, lines 18-21).

The claimed invention, as set forth in claim 11, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, is also directed to a firewall apparatus for selectively passing protocols and services (page 7, lines 22-24). The apparatus may comprise an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy (page 7, line 24 to page 8, line 4). The apparatus may also comprise a key exchanger for exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy (page 8, lines 4-10). The apparatus may further comprise a requestor for requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second

encryption key and in accordance with the second security policy (page 8, lines 10-14). The apparatus may still further comprise a decryptor for decrypting encrypted data, using the first encryption key (page 8, lines 15-18). The apparatus may still further comprise a filter for applying a predetermined filtering policy to the decrypted data (page 8, lines 15-18).

The claimed invention, as set forth in claim 12, and as described and shown in the specification and Figures 1-5 of the above-identified patent application, respectively, may further comprise an encryptor for re-encrypting the decrypted data.

GROUNDS OF REJECTION ON APPEAL

Claims 1, 2, 4-8, and 10-12 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Perlman et al. (U.S. Patent No. 6,546,486).

Claims 3 and 9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Perlman et al. (U.S. Patent No. 6,546,486) in view of Ylonen et al. (U.S. Patent No. 6,438,612).

ARGUMENT

The Appellants respectfully appeal the decision of the Examiner to finally reject claims 1-12 of the above-identified patent application. As discussed below, it is respectfully

submitted that the Examiner has failed to establish a prima facie case of anticipation or obviousness against the appealed claims.

I. THE EXAMINER HAS FAILED TO ESTABLISH A PRIMA FACIE CASE OF ANTICIPATION AGAINST CLAIMS 1, 2, 4-8, AND 10-12

The Examiner asserts that claims 1, 2, 4-8, and 10-12 are anticipated by Perlman et al. (U.S. Patent No. 6,546,486) under 35 U.S.C. § 102(e).

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id.. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). "Such possession is effected if one of ordinary skill in the art could have combined the publication's

description of the invention with his own knowledge to make the claimed invention." Id..

Regarding claim 1, the Examiner asserts that Perlman et al. discloses the claimed invention. Applicants respectfully disagree. Specifically, Applicants respectfully submit that Perlman et al. fails to teach, or even suggest, the steps of detecting an exchange of a first encryption key between a host device and a remote device, and exchanging a second encryption key with the host device, as claimed.

The Examiner asserts that the claimed "second key" is disclosed by the firewall public key of Perlman et al. (see Office Action dated February 28, 2006 at p. 2). However, Applicants respectfully submit that if the claimed "second key" is the firewall public key, then Perlman fails to disclose detecting an exchange of a first encryption key between a host device and a remote device, as claimed. Indeed, the Examiner relies on col. 4, lines 63-66, to allegedly disclose this feature. That is, the cited portion refers to "message key 204" for use in encrypting a message between source 102 and destination 110. However, as disclosed in Perlman et al. (and relied upon by the Examiner) it is message key 306 that is detected (see col. 5, lines 55-67). Key 204 (i.e., the alleged claimed "first key") is not detected, but rather is passed to

destination 110 for decryption at the destination. Therefore, even if the "public key" disclosed by Perlman et al. is considered to be the claimed "second key," then Perlman et al. fails to disclose the claimed features of the "first key."

The Examiner also asserts, in the Advisory Action dated June 7, 2006, that the key 204 is "detected as it passes through the firewall and when it receives the security association (Perlman, column 5 lines 1-6)" by relying on the assertion that "message key 306 is detected by the firewall as it is exchanged between source and destination through the firewall (Perlman, column 5 lines 54-56)." The Examiner acknowledges that Perlman et al. does not teach that key 204 is detected. Rather, the basis for the Examiner's assertion appears to be that since key 204 is "merely one embodiment of the invention" and key 306 is presumably detected in a "second embodiment", the keys are, in effect, interchangeable with each other. However, Applicants respectfully disagree. Specifically, Applicants respectfully submit that the Examiner's picking and choosing of components from differing embodiments of Perlman et al. is improper. For example, key 204 disclosed by Perlman et al. is directed to an embodiment where content screening is within a firewall that encrypts a message 202 with a message key 204 for "a single packet, or alternatively a group of packets that collectively

form a single message" (see Perlman et al. at col. 4, lines 56-62; Fig. 2). On the other hand, key 306 is directed to a different embodiment where the message is a "self-contained message" (see Perlman et al. at col. 5, lines 38-54; Fig. 3). Furthermore, even assuming that Examiner's picking and choosing of components from different embodiments of Perlman et al. is proper, Applicants respectfully submit that there is no disclosure, teaching, or suggestion to permit such an interchangeability of parts. In fact, Perlman et al. discloses separate embodiments to describe and emphasize different features and functionalities of content screening "in more detail" based on separate and distinct embodiments. As discussed above, the keys of Perlman et al. serve different purposes. Key 204 is not detected, but rather is passed to destination 110 for decryption at the destination. Thus, if the "public key" disclosed by Perlman et al. is considered to be the claimed "second key," then Perlman et al. fails to disclose the claimed features of the "first key." As a result, the alleged detection of key 306 does not suffice to teach or suggest that key 204 is detected.

In view of the foregoing, it is respectfully submitted that Perlman et al. fails to teach, or even suggest, the claimed invention as set forth in claim 1. Thus, is it further

respectfully submitted that claim 1 is allowable over Perlman et al..

Claim 2 is dependent upon independent claim 1. Thus, since independent claim 1 should be allowable as discussed above, claim 2 should also be allowable at least by virtue of its dependency on independent claim 1. Moreover, claim 2 recites additional features which are not disclosed, or even suggested, by Perlman et al.. For example, claim 2 recites not allowing encrypted data to pass when it is determined that the first encryption key is not received. Perlman et al. fails to disclose, or even suggest, such claimed features.

Regarding claims 4, 5, 7, 10, and 11, these claims recite subject matter related to claim 1. Thus, the arguments set forth above with respect to claim 1 are equally applicable to claims 4, 5, 7, 10, and 11. Accordingly, is it respectfully submitted that claims 4, 5, 7, 10, and 11 are allowable over Perlman et al. for the same reasons as set forth above with respect to claim 1.

Claims 6, 8, and 12 are dependent upon independent claims 5, 7, and 11, respectively. Thus, since independent claims 5, 7, and 11 should be allowable as discussed above, claims 6, 8, and 12 should also be allowable at least by virtue of their dependency on independent claims 5, 7, and 11. Moreover, these

claims recite additional features which are not disclosed, or even suggested, by Perlman et al.. For example, claim 8 recites an encrypted data blocker for not allowing encrypted data to pass when it is determined that the first encryption key is not received. Perlman et al. fails to disclose, or even suggest, such claimed features.

In view of the foregoing, it is respectfully submitted that Perlman et al. fails to disclose, or even suggest, the elements of claims 1, 2, 4-8, and 10-12. Accordingly, it is respectfully submitted that claims 1, 2, 4-8, and 10-12 of the present application are not anticipated by Perlman et al., and thus the Examiner has failed in his duty to establish at least a prima facie case of anticipation against claims 1, 2, 4-8, and 10-12 of the present application. Therefore, it is respectfully requested that the anticipation rejection of claims 1, 2, 4-8, and 10-12 be withdrawn.

II. THE EXAMINER HAS FAILED TO ESTABLISH A PRIMA FACIE CASE OF OBVIOUSNESS AGAINST CLAIMS 3 AND 9

The Examiner asserts that claims 3 and 9 are unpatentable over Perlman et al. (U.S. Patent No. 6,546,486) in view of Ylonen et al. (U.S. Patent No. 6,438,612) under 35 U.S.C. § 103(a).

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). The Patent Office can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of references. Id.. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). That is, under 35 U.S.C. § 103, teachings of references can be combined only if there is some suggestion or motivation to do so. Id.. However, the motivation cannot come from the applicant's invention itself. In re Oetiker, 977 F.2d 1443, 1447, 24 USPQ2d 1443, 1446 (Fed. Cir. 1992). Rather, there must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the art would make the combination. Id..

It is respectfully submitted that the obviousness rejection of claims 3 and 9 has become moot in view of the deficiencies of the primary reference Perlman et al. as discussed above with respect to independent claims 1 and 7, respectively. That is,

claims 3 and 9 are dependent upon independent claims 1 and 7, respectively, and thus inherently incorporate all of the limitations of independent claims 1 and 7, respectively. Also, the secondary reference Ylonen et al. fails to disclose, or even suggest, the deficiencies of the primary reference Perlman et al. as discussed above with respect to independent claims 1 and 7. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary reference Ylonen et al. with the primary reference Perlman et al. also fails to disclose, or even suggest, the deficiencies of the primary reference Perlman et al. as discussed above with respect to independent claims 1 and 7. Accordingly, claims 3 and 9 should be allowable over the combination of the secondary reference Ylonen et al. with the primary reference Perlman et al. at least by virtue of their dependency on independent claims 1 and 7. Moreover, claims 3 and 9 recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination. For example, claims 3 and 9 recite detecting an exchange of a first encryption key by monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged. Perlman et al. and Ylonen et al., either alone or in combination, fail to disclose, or even

suggest, such claimed features, particularly when viewed in combination with the features of independent claims 1 and 7.

In view of the foregoing, it is respectfully submitted that the combination of the primary reference Perlman et al. with the secondary reference Ylonen et al. fails to disclose, or even suggest, the elements of claims 3 and 9. Accordingly, it is respectfully submitted that claims 3 and 9 of the present application are not unpatentable over the combination of the primary reference Perlman et al. with the secondary reference Ylonen et al., and thus the Examiner has failed in his duty to establish at least a prima facie case of obviousness against claims 3 and 9 of the present application. Therefore, it is respectfully requested that the obviousness rejection of claims 3 and 9 be withdrawn.

CONCLUSION

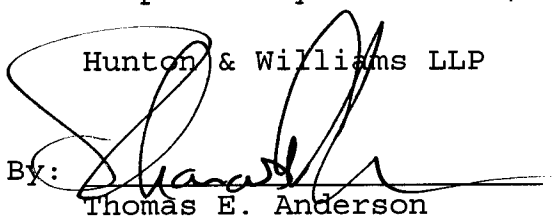
In view of the foregoing, it is respectfully submitted that the Examiner has failed to establish a prima facie case of anticipation or obviousness against the appealed claims. Thus, it is respectfully submitted that the final rejection of claims 1-12 is improper and the reversal of same is clearly in order and respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-0206, and please credit any excess fees to such deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: 
Thomas E. Anderson
Registration No. 37,063

TEA/vrp

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: April 26, 2007

CLAIMS APPENDIX

1 (Previously Presented). A method for enabling a firewall to securely pass encrypted data, the method comprising:

detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device; wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

passing encrypted data when it is determined that the first encryption key is received.

2 (Original). The method of claim 1, further comprising:

not allowing encrypted data to pass when it is determined that the first encryption key is not received.

3 (Original). The method of claim 1, wherein the step of detecting an exchange of a first encryption key further comprises:

monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged.

4 (Previously Presented). A method for enabling a firewall to selectively monitor encrypted data traffic, the method comprising:

detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key enables confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

exchanging a second encryption key with the host device when the exchange of the first key is detected, wherein the exchange of the second encryption key enables confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

decrypting encrypted data, using the first encryption key, according to a predetermined monitoring policy.

5 (Previously Presented). A method for enabling a firewall to selectively pass protocols and services, the method comprising:

detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host

device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy;

decrypting encrypted data, using the first encryption key; and

applying a predetermined filtering policy to the decrypted data.

6 (Original). The method of claim 5, further comprising:

re-encrypting the decrypted data.

7 (Previously Presented). A firewall apparatus that securely passes encrypted data, the apparatus comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second

security policy;

a key requestor for requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device; wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

an encrypted data passer for passing encrypted data when it is determined that the first encryption key is received.

8 (Original). The apparatus of claim 7, further comprising:

an encrypted data blocker for not allowing encrypted data to pass when it is determined that the first encryption key is not received.

9 (Original). The apparatus of claim 7, wherein the exchange detector further comprises:

a monitor for monitoring Internet Key Exchange (IKE) protocol data traffic to determine whether the first encryption key is exchanged.

10 (Previously Presented). A firewall apparatus for selectively monitoring encrypted data traffic, the apparatus comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device, wherein the first encryption key enables confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the first key is detected, wherein the exchange of the second encryption key enables confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

a requestor for requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy; and

a decryptor for decrypting encrypted data, using the first encryption key, according to a predetermined monitoring policy.

11 (Previously Presented). A firewall apparatus for selectively passing protocols and services, the method comprising:

an exchange detector for detecting an exchange of a first encryption key between a host device and a remote device,

wherein the first encryption key supports confidentiality protection of first data exchanged between the host device and the remote device according to a first security policy;

a key exchanger for exchanging a second encryption key with the host device when the exchange of the first encryption key is detected, wherein the exchange of the second encryption key supports confidentiality protection of second data exchanged between the firewall and the host device according to a second security policy;

a requestor for requesting at the firewall, based at least in part upon the second security policy, the first encryption key from the host device, wherein the first encryption key is sent under the protection of the second encryption key and in accordance with the second security policy;

a decryptor for decrypting encrypted data, using the first encryption key; and

a filter for applying a predetermined filtering policy to the decrypted data.

12 (Original). The apparatus of claim 11, further comprising:

an encryptor for re-encrypting the decrypted data.

EVIDENCE APPENDIX

[NONE]

RELATED PLEADINGS APPENDIX

[NONE]